Claims

What is claimed is:

1. A method for secure generation of a seed for use in performing one or more cryptographic operations, the method comprising the steps of:

a seed generation server providing a first string to a seed generation client;

the seed generation client generating a second string, encrypting the second string utilizing a key, and sending the encrypted second string to the seed generation server;

the seed generation client generating the seed as a function of at least the first string and the second string; and

the seed generation server decrypting the encrypted second string and independently generating the seed as a function of at least the first string and the second string.

2. The method of claim 1 wherein the seed comprises a symmetric key.

3. The method of claim 1 wherein the seed is generated, by at least one of the seed generation client and the seed generation server, as a function of a combination of the second string and one or more of: (i) the first string, and (ii) identifying information associated with the seed generation server.

4. The method of claim 3 wherein the identifying information associated with the seed generation server comprises a public key of the seed generation server.

5. The method of claim 1 wherein the key utilized by the seed generation client to encrypt the second string comprises a public key of the seed generation server.

6. The method of claim 1 wherein the key utilized by the seed generation client to encrypt the second string comprises a secret key shared by the seed generation client and the seed generation server.

7. The method of claim 1 wherein the seed generation client comprises or is otherwise associated with an authentication token.

8. The method of claim 1 wherein the seed generation server comprises or is otherwise associated with an authentication entity.

9. The method of claim 1 wherein the seed generation server sends an authentication code to the seed generation client, the authentication code proving knowledge of the generated seed and instructing the seed generation client to store the generated seed.

10. The method of claim 9 wherein the authentication code is cryptographically derived from a secret key shared by the seed generation client and the seed generation server.

11. The method of claim 1 wherein the seed generation server sends the generated seed to an authentication entity.

12. The method of claim 11 wherein the seed generation server also sends user identifying information associated with the seed to the authentication entity.

13. The method of claim 1 wherein the seed generation client is associated with a first processing device and the seed generation server is associated with a second processing device.

14. The method of claim 1 wherein the seed generation client and the seed generation server communicate with one another through at least one intermediary processing device.

15. The method of claim 1 wherein the seed generation server initiates the seed generation process responsive to receipt of a management command.

16. The method of claim 1 wherein the seed generation server initiates the seed generation process responsive to receipt of a request initiated by the seed generation client.

17. The method of claim 16 wherein the seed generation client in response to initiation of the seed generation process by the seed generation server provides the seed generation server with information indicating one or more processing algorithms suitable for use in the seed generation process.

18. The method of claim 17 wherein the seed generation server responsive to the information indicating one or more processing algorithms provides to the seed generation client additional information specifying one or more characteristics of the seed generation process.

19. The method of claim 1 wherein the second string comprises a combination of at least two component strings, including at least a first component generated in the seed generation client by interaction with the seed generation server and a second component previously stored in the seed generation client.

20. The method of claim 1 wherein the seed is generated by repeatedly applying a cryptographic algorithm to successive portions of an additional string generated utilizing the first string, the second string and the key.

21. The method of claim 20 wherein the additional string generated utilizing the first string, the second string and the key comprises a concatenation of the first string, the second string and the key.

22. The method of claim 20 wherein the additional string comprises *n* portions C[1], C[2], . . . C[*n*], and the seed is generated by computing:

I[1] = Algorithm (C[1], C[2])
I[2] = Algorithm (I[1], C[3])
. . .
I[*n*-1] = Algorithm (I[*n*-2], C[*n*])
seed = I[*n*-1],

where Algorithm (A, B) denotes application of the cryptographic algorithm to portion B of the string utilizing an algorithm parameter denoted by A.

23. The method of claim 20 wherein the cryptographic algorithm comprises a one-way cryptographic operation.

24. The method of claim 23 wherein the one-way cryptographic operation comprises a hash function.

25. The method of claim 20 wherein the cryptographic algorithm comprises an encryption operation.

26. The method of claim 25 wherein the encryption operation comprises the AES algorithm.

27. The method of claim 1 wherein the seed generation client stores the generated seed in an authentication token.

28. The method of claim 1 wherein the seed generation server stores the generated seed in an authentication entity.

29. The method of claim 1 wherein the generated seed is used to replace an existing seed known to both the seed generation client and the seed generation server.

30. The method of claim 29 wherein the generated seed is used to replace an existing seed in an authentication token associated with the seed generation client and in an authentication entity associated with the seed generation server.

31. The method of claim 30 wherein the authentication token replaces the existing seed with the generated seed after the receipt of a signal from the authentication entity.

32. The method of claim 31 wherein the signal from the authentication entity comprises an authentication code cryptographically derived from the seed.

33. The method of claim 30 wherein the authentication entity replaces the existing seed with the generated seed after receipt of a signal from the authentication token.

34. The method of claim 33 wherein the signal from the authentication token comprises an authentication code cryptographically derived from the seed.

35. An apparatus for secure generation of a seed for use in performing one or more cryptographic operations, the apparatus comprising:

a processing device comprising a processor coupled to a memory, the processing device implementing at least one of a seed generation client and a seed generation server;

wherein the seed generation server provides a first string to the seed generation client;

the seed generation client generates a second string, encrypts the second string utilizing a key, and sends the encrypted second string to the seed generation server;

the seed generation client generates the seed as a function of at least the first string and the second string; and

the seed generation server decrypts the encrypted second string and independently generates the seed as a function of at least the first string and the second string.

36. A machine-readable storage medium containing one or more software programs for secure generation of a seed for use in performing one or more cryptographic operations, wherein the one or more software programs when executed by a processing device implement at least one of a seed generation client and seed generation server;

wherein the seed generation server provides a first string to the seed generation client;

the seed generation client generates a second string, encrypts the second string utilizing a key, and sends the encrypted second string to the seed generation server;

the seed generation client generates the seed as a function of at least the first string and the second string; and

the seed generation server decrypts the encrypted second string and independently generates the seed as a function of at least the first string and the second string.

37. A method for secure generation of a seed for use in performing one or more cryptographic operations, the method being implemented in a seed generation client, the method comprising the steps of:

receiving a first string from a seed generation server;

generating a second string, encrypting the second string utilizing a key, and sending the encrypted second string to the seed generation server; and

generating the seed as a function of at least the first string and the second string.

38. An apparatus for secure generation of a seed for use in performing one or more cryptographic operations, the apparatus comprising:

a processing device comprising a processor coupled to a memory, the processing device implementing a seed generation client;

the seed generation client being configured: (i) to receive a first string from a seed generation server; (ii) to generate a second string, to encrypt the second string utilizing a key, and to send the encrypted second string to the seed generation server; and (iii) to generate the seed as a function of at least the first string and the second string.

39. A method for secure generation of a seed for use in performing one or more cryptographic operations, the method being implemented in a seed generation server, the method comprising the steps of:

providing a first string to a seed generation client;

receiving from the seed generation client a second string encrypted utilizing a key;

decrypting the encrypted second string; and

generating the seed as a function of at least the first string and the second string.

40. An apparatus for secure generation of a seed for use in performing one or more cryptographic operations, the apparatus comprising:

a processing device comprising a processor coupled to a memory, the processing device implementing a seed generation server;

the seed generation server being configured: (i) to provide a first string to a seed generation client; (ii) to receive from the seed generation client a second string encrypted utilizing a key; (iii) to decrypt the encrypted second string; and (iv) to generate the seed as a function of at least the first string and the second string.